事例で学ぶセキュリティインシデント（第17回）

暗号ファイルとパスワードを別メールで送るPPAPのリスク

2024.10.15

関西で日用品を製造・販売するQ社の商品企画担当者からIT担当者に電話があった。「まだ発表前の新商品情報が外部に漏れているようです。私たちと一緒に調べてもらえませんか」。新商品の製造準備のため、工場の製造課長にいつものように「PPAP」で製品仕様書の添付ファイルをメールで送信したという。「危惧していたが、PPAPの添付ファイルから情報が盗まれた可能性もある」とIT担当者はつぶやいた。

悪意のある第三者に添付ファイルが盗聴される恐れも

PPAPは添付ファイルをZIP暗号化してメール送信した後、別メールで暗号を復号するためのパスワードを送信する仕組み。長らく、メールセキュリティの手段の1つとして企業や官公庁などでも利用されてきた。だが、2020年頃に当時のデジタル改革担当大臣が内閣府でのPPAP廃止を宣言したことから話題となり、民間企業でもPPAPを廃止する動きが広がった経緯がある。

では、PPAPの何が危ないのか。1つは、暗号化した添付ファイルとパスワードを別のメールとはいえ同一経路で送信することから、悪意のある第三者に盗聴される恐れがあるためだ。また、添付ファイルを暗号化してメール送信するので、受信側のウイルスチェック機能が働かない可能性がある。万一、ウイルスがZIPファイルに紛れ込んでいた場合、メールの受信者はウイルス感染する恐れもある。

そして、悪意のある第三者にメールを盗聴されないまでも、メールの誤送信で社内・社外の無関係の人にメールが送られる危険性もある。その人にパスワードを記載したメールも届くため、情報漏えいの原因にもなりかねないリスクがあるのだ。

加えて、メールの送受信にかかわる手間が増える問題もある。添付ファイルを送信する際、ファイルの暗号化とともに、別メールでのパスワード送信を自動化するツールもあるが、受信側は添付ファイルの復号化のためにパスワードを入力(コピー&ペースト)する必要がある。セキュリティ確保のために仕方がないと思いつつ、添付ファイルを開く人もいるのではないだろうか。

非公開の情報を見た会社から取引を持ちかけられる… 続きを読む